UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/640,606	08/17/2000	Rajeev Khanolkar	26836.701.201	4499

21971 7590 10/18/2005

WILSON SONSINI GOODRICH & ROSATI
650 PAGE MILL ROAD
PALO ALTO, CA 94304-1050

EXAMINER	
ARANI, TAGHI T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/640,606	**Applicant(s)** KHANOLKAR ET AL.	
	Examiner Taghi T. Arani	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-36 have been examined and are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.1 14, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.1 14, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on 7/22/2005 has been entered.

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.

Response to Amendment

4. Applicant's amendment filed 7/22/2005 necessitated the new ground(s) of rejection presented in this Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 25, 35 and 36 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,839,850 to Campbell et al. (hereinafter Campbell).

As per claims 1, Campbell teaches an event parser in communication with multiple network service devices (col. 5, lines 35-41,i.e. SI&W Engine receives audit information from Audit Agents (AAs), see col. 12, lines 58-67, where AUDIT process 306 parses the audit information, see also Fig. 1 and associated text), the event parser being able to receive log data in real time from the device (col. 6, lines 8-10, SI&W Engine indicating in near real-time that a potential security threats exist), the log data including information detailing a network intrusion event received from the network service device if an intrusion has occurred, the event parser being able to parse the information to create a corresponding event object concerning the intrusion event (col. 12, lines 29-44, SI &W Engine maps events in the audit stream into key SI&W events and updates the associated gauges, see also col. 13, lines 58-67);

an event manager in communication with the event parser, the event manager being able to receive the event object, the event manager being configured to evaluate the event object according to at least one predetermined threshold condition such that (col. 13, lines 46-57), when the event object satisfies the predetermined threshold condition, the event manager designates the event object to be broadcast in real time (col. 14, lines 21-39, where HADES 308 evaluates indicators to ultimately determine whether a potential threat exists and whether to produce a warning);

an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event object as an intrusion alarm (col. 12, lines 45-53, i.e. SIW process 310 which communicates with external processes on the audit server to cause a warning message to be displayed for the ISO when warning is produced by the analysis function); and

means for alerting the user that a network intrusion event has occurred (i.e. a warning message to be displayed for the ISO when warning is produced by the analysis function).

As per claim 35, Campbell teaches a computer system for detecting and monitoring network intrusion events from log data received from network service devices in a computer network, the computer system having discrete modules associated with a function performed on the log data received, the computer system comprising (Abstract):

an event parser in communication with multiple network service devices, the event parser being able to receive log data in real time from the devices, the log data including information detailing a network intrusion event received from the network service devices if an intrusion has occurred, the event parser being able to parse the information to create corresponding event objects concerning the intrusion events (col. 5, lines 35-41,i.e. SI&W Engine receives audit information from Audit Agents (AAs) , see col. 12, lines 58-67, where AUDIT process 306 parses the audit information, see also Fig. 1 and associated text);

an event aggregator, the event aggregator being able to filter the event objects based on event type and severity (col. 5, line 66-col. 6, line10);

an event manager in communication with the event aggregator, the event manager being able to receive the event object, the event manager being configured to evaluate the event object according to at least one predetermined threshold condition such that (col. 13, lines 46-57), when the event object satisfies the predetermined threshold condition, the event manager designates the event object to be broadcast in real time (col. 14, lines 21-39, where HADES 308 evaluates indicators to ultimately determine whether a potential threat exists and whether to produce a warning);

an event broadcaster in communication with the event manager for receiving event objects designated-by the event manager for broadcast, the event broadcaster being able to transmit the event object in real time relative to the receipt of the log data, as an intrusion alarm (col. 12, lines 45-53, i.e. SIW process 310 which communicates with external processes on the audit server to cause a warning message to be displayed for the ISO when warning is produced by the analysis function); and

means for alerting the user that a network intrusion event has occurred (a warning message to be displayed for the ISO when warning is produced by the analysis function).

As per claims 25 and 36, Campbell teaches a method for detecting and monitoring network intrusion events from log data received from network service devices in a computer network, wherein the network service devices comprise a device from a group-comprising a firewall, VPN (virtual private network) server or router, and e-mail server (Figure 1 ans associated text, also col. 7, line 65 through col. 8, line 41, i.e. the network includes a workstation , network server, host computer , terminal, personal computer , an Audit Server and a firewall which connects the secure network to an interface or an IP protocol router) comprising the steps of (Abstract):

receiving log data in real time from multiple network security devices, the log data including information detailing at least network intrusion events received from the network service devices (col. 5, lines 35-41,i.e. SI&W Engine receives audit information from Audit Agents (AAs));

parsing the log data information to create corresponding event objects (col. 12, lines 58-67, where AUDIT process 306 parses the audit information, see also Fig. 1 and associated text);

filtering the event objects based on event type and severity (col. 13, lines 46-57, i.e. SI &W Engine maintains a separate Gauge Set for each monitored user and machine and evaluates concern levels for individual users and the network nodes); and

evaluating the event objects according to at least one predetermined threshold condition (col. 13, lines 46-57, The SI &W Engine uses a Hierarchical aggregation of information collected in the gauges and the gauges are evaluated to determine whether significant threshold of user activity have been reached , see also col. 14, lines 12-20);

where the information contained within an event object satisfies the predetermined threshold condition, broadcasting the event object as an intrusion alarm in real time, relative to the receipt of the log data, to a display screen on a graphic user interface (col. 10, lines 50-61, see also col. 12, lines 45-53, i.e. SIW process 310 which communicates with external processes on the audit server to cause a warning message to be displayed for the ISO when warning is produced by the analysis function) .

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-10, 12-15, 17-22, 25-31, 33 and 34 rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, USP 6,070,244 to Orchier et al (hereinafter " Orchier") and further in view of U.S. Patent 6,839,850 to Campbell et al. (hereinafter Campbell).

As per claim 1, Orchier teaches an event parser in communication with at least one network service device, the event parser being able to receive log data in real time from the device, the log data including information detailing a network intrusion event received from the network service device if an intrusion has occurred, the event parser being able to parse the information to create a corresponding event object concerning the intrusion event (column 4, lines 5-10);

an event manager in communication with the event parser, the event manager being able to receive the event object, the event manager being configured to evaluate the event object according to at least one predetermined threshold condition such that, when the event object satisfies the predetermined threshold condition, the event manager designates the event object to be broadcast in real time (column 4, lines 10-21);

Orchier teaches an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event object as an intrusion alarm; and means for alerting the user that a network intrusion event has occurred (column 4, lines 27-30).

Orchier fails to teach transmitting the event object in real time, relative to the receipt of the log data, as an intrusion alarm.

However Campbell teaches a security Indication and warning (SI &W) Engine capable of indicating that a potential security threat exists in real-time (Abstract, Figure 4 and associated text, see also col. 13, lines 33 through col. 14, line 39 for detailed disclosure of SI &W Engine)

Campbell further teaches transmitting the event object in real time, relative to the receipt of the log data, as an intrusion alarm (see col. 13, lines 25-32, Fig. 4 and associated text, see also col. 12, lines 28-53).

It would have been obvious to one of ordinary skill in the art to modify the Orchier's event broadcaster to that of Campbell's real time intrusion detection and misuse system to allow recognition of suspicious behavior as it occurs and to permit the information security officer to respond to the behavior quickly enough to effectively counter a possible security threat (Campbell, col. 9, line 66 through col. 10, line 3).

As per claim 25, Orchier teaches a method for detecting and monitoring network intrusion events from log data received from network service devices in computer network, wherein the network service device comprises a device from a group comprising a firewall, VPN (virtual private network) server or router , and e-mail server comprising the step of :

receiving log data in real time, the log data including information detailing at least one network intrusion event received from the at least one network service devices, wherein the network service devices comprise a device from a group comprising a firewall, VPN (virtual private network) server or router, and e-mail server (column 4, lines 1-10, lines 32-47, where security domains represent workstations, servers, LANs, Windows NT and other such computer software or hardware, i.e. firewall, router, and e-mail server);

parsing the log data information to create a corresponding event objects (column 4, lines 10-21);

evaluating the event objects according to at least one predetermined threshold condition (column 4, lines 27-30);

where the information contained within the event objects satisfies the predetermined threshold condition, broadcasting the event object as an intrusion alarm to a display screen on a graphic user interface (column 13, lines 10-12).

Orchier teaches an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event object as an intrusion alarm; and means for alerting the user that a network intrusion event has occurred (column 4, lines 27-30).

Orchier fails to teach transmitting the event object in real time, relative to the receipt of the log data, as an intrusion alarm.

However Campbell teaches a security Indication and warning (SI &W) Engine capable of indicating that a potential security threat exists in real-time (Abstract, Figure 4 and associated text, see also col. 13, lines 33 through col. 14, line 39 for detailed disclosure of SI &W Engine)

Campbell further teaches transmitting the event object in real time, relative to the receipt of the log data, as an intrusion alarm (see col. 13, lines 25-32, Fig. 4 and associated text, see also col. 12, lines 28-53).

It would have been obvious to one of ordinary skill in the art to modify the Orchier's event broadcaster to that of Campbell's real time intrusion detection and misuse system to allow recognition of suspicious behavior as it occurs and to permit the information security officer to respond to the behavior quickly enough to effectively counter a possible security threat (Campbell, col. 9, line 66 through col. 10, line 3).

As per claim 2, Orchier teaches alerting the user that a network intrusion event has occurred is a graphical user interface in communication with the event broadcaster, the graphical user interface comprising a display screen for displaying an intrusion alarm and the information contained within the corresponding event object received from the event broadcaster (column 13, lines 10-12).

As per claims 3 and 26, Orchier teaches:

means for storing event objects, said means coupled to the event parsers (column 5, lines 30-40);

a report servlet coupled to the graphic user interface, the report servlet for recalling stored event objects in response to user queries from the graphic user interface and displaying recalled event objects on the graphic user interface display screen (column 13, lines 42-44);

an application reporter coupled to the report servlet for receiving and processing user queries and for performing searches of stored event objects (column 13, lines 42-44); and

a database accessible by the application reporter, for holding stored event objects, the database configured to recall event objects in response to searches executed by the application reporter (column 5, lines 30-40).

As per claim 4 and 27, Orchier teaches:

a network port to receive log data having a conforming message format from at least one network service device (column 4, lines 19-21);

means for transmitting the log data having a conforming message format to the event parsers, said means coupled to the network port (column 4, lines 510);and

a reporting agent coupled to the network port for collecting log data having a nonconforming message format from the at least one network service device and converting the log data to a conforming message format (column 4, lines 710).

As per claims 5 and 28, Orchier teaches the conforming message format is syslog (column 13, line 50).

As per claim 6, Orchier teaches the graphical user interface display screen comprises an alarm console, coupled to the event broadcaster, configured to display intrusion alarms, and a report console, coupled to the report servlet, configured to execute queries input by a user and display results, wherein the alarm console and event broadcaster are displayed simultaneously on the display screen (column 14, lines 5-10 and Fig 8b).

As per claims 7 and 30, Orchier teaches the report console is further configured to display query result data in summary lines, said summary lines comprising hypertext links providing access to further data (column 13, lines 4550 and Fig 8b, 'Note').

As per claims 8 and 29, Orchier teaches the alarm console displays intrusion alarms in summary lines, said summary lines comprising hypertext links providing access to further data (column 13, lines 45-50 and Fig 8b, 'Note').

As per claim 9, Orchier teaches the graphical user interface displays the status of network security devices in real time (column 2, lines 30-35).

As per claim 10, Orchier teaches the graphical user interface displays the status of network security devices in summary lines, said summary lines comprising hypertext links providing access to further data (column 13, lines 4548 and Fig 8b, `Note').

As per claims 12, 33, and 34, Orchier teaches comprising a chat manager accessible to a user from the alarm console for executing electronic communications links between the user and others having an electronic communications link to the computer system (column 13, lines 10-15 and column 14, lines 5-10).

As per claim 13, Orchier teaches the electronic communications link is an on line link established through a web browser interface (column 13, lines 35-52).

As per claim 14, Orchier teaches a plurality of event parsers wherein each event parser is configured to receive log data from a predetermined network service device, the plurality of parsers each coupled to the event manager (column 4, lines 1-5).

As per claim 15, Orchier that teaches the information contained within the event object is read by the event manager and assigned a severity level corresponding to the event type information contained within the event object,
and the predetermined threshold condition is the assigned severity level (column 13, lines 24-28 and column 13, lines 65-66).

As per claim 17, Orchier teaches an event aggregator module and wherein the event parser is housed within the event aggregator module, and log data from a multiplicity of network device sources is received by the event parser (Figure 2, element 54).

As per claim 18, Orchier teaches the event parser reads log data posted in extensible markup language (column 13, lines 45-55).

As per claim 19, Orchier teaches the computer system is one of a multiplicity of computer systems each having a graphic user interface and the computer system further comprises a central graphic user interface which, accesses at least one of the graphic user interfaces of the multiplicity of computer systems (column 5, lines 19-25).

As per claim 20, Orchier teaches the central graphic user interface accesses at least one of the report servlets of the multiplicity of computer systems and communicates with at least one of the databases of the multiplicity of computer systems (column 5, lines 19-25 and column 7, lines 28-50).

As per claim 21, Orchier teaches filtering event objects received by the event manager according to one or more predetermined conditions so as to restrict the field of event objects designated for broadcast (column 4, lines 19-30 and column 13, lines 32-35).

As per claims 22 and 31, Orchier teaches filtering log data received at the network port according to one or more predetermined conditions so as to restrict receipt of corresponding log data by said transmitting means (column 13, lines 55-67).

Claim Rejections - 35 USC § 103

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orchier and Campbell in view of Battat et al, herein Battat, (USP 5,958,012).

As per claim 11, Orchier does not teaches the graphical user interface displays the status of network security devices in a color-coded format where said color designates a particular status level for the particular device. Battat teaches displaying displays the status of network security devices in a color coded format where said color designates a particular status level for the particular device (column 5, lines 5-7). Battat uses a color-coded status level so that events that need immediate attention are quickly spotted first. It would be advantageous to act upon the most severe threat first.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Battat within the system of Orchier because it would allow the events to be color-coded which would help the administrator to differentiate between severe threats and minor threats. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orchier and Campbell in view of Hill et al, herein Hill, (USP 6,088,804).

As per claim 16, Orchier fails to teach that the severity level is one of seven categories for types of events contained within event objects. Hill teaches categorizes types of events into more than one category (column 14, lines 26-29).

Categorizing types of events is advantageous because it would allow the user to quickly identify the severity level of the problem.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Hill within the system of Orchier because it would allow the events to be categorized, which would help the administrator to differentiate between severe threats and those threats of less importance. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

8. **Claims 23, 24, and 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over Orchier and Campbell.

As per claims 23, 24, and 32, Orchier teaches the predetermined conditions are application name, host name, and internal device alarm identification (column 13, lines 55-66).

Orchier teaches retrieving data by various network domain parameters. Orchier is silent in expressly disclosing using the source address, destination address, destination port, and protocol. Orchier's computer system without a doubt does log these types of parameters, as any network monitoring system would need to log, in order to adequately monitor and protect the entire network. Since these types of parameters are being logged, it would have been obvious to one of ordinary skill in the art to also use these parameters as conditions in which to retrieve crucial network data.

In view of this it would have been obvious to one of ordinary skill in the art to modify the teachings of Orchier by also using the source address, destination address, destination port, and protocol to retrieve log data about an event.

Conclusion

Prior arts made of record, not relied upon:

US 2002/0093527 to Sherlock et al.

US 2005/0185673 to Campbell et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100